Title (en)

SYSTEM AND METHOD FOR HIGH SPEED THREAT INTELLIGENCE MANAGEMENT USING UNSUPERVISED MACHINE LEARNING AND PRIORITIZATION ALGORITHMS

Title (de)

SYSTEM UND VERFAHREN ZUR HOCHSCHNELLEN BEDROHUNGSINTELLIGENZVERWALTUNG MITHILFE UNÜBERWACHTEM MASCHINENLERNEN UND PRIORISIERUNGSALGORITHMEN

Title (fr)

SYSTÈME ET PROCÉDÉ DE GESTION À GRANDE VITESSE DE RENSEIGNEMENTS SUR LES MENACES À L'AIDE D'ALGORITHMES NON SUPERVISÉS D'APPRENTISSAGE AUTOMATIQUE ET DE HIÉRARCHISATION

Publication

EP 3143547 B1 20190320 (EN)

Application

EP 15788313 A 20150724

Priority

SG 2015050233 W 20150724

Abstract (en)

[origin: WO2017018926A1] This document discloses a system and method for consolidating threat intelligence data for a computer and its related networks. Massive volumes of raw threat intelligence data are collected from a plurality of sources and are partitioned into a common format for cluster analysis whereby the clustering of the data is done using unsupervised machine learning algorithms. The resulting organized threat intelligence data subsequently undergoes a weighted asset based threat severity level correlation process. All the intermediary network vulnerabilities of a particular computer network are utilized as the critical consolidation parameters of this process. The final processed intelligence data gathered through this high speed automated process is then formatted into predefined formats prior to transmission to third parties.

IPC 8 full level

G06F 21/56 (2013.01); **G06K 9/62** (2006.01); **G06N 20/00** (2019.01); **H04L 29/06** (2006.01)

CPC (source: EP US)

G06F 18/2321 (2023.01 - EP US); **G06F 18/24147** (2023.01 - EP US); **G06F 21/56** (2013.01 - EP US); **G06N 20/00** (2018.12 - EP US); **H04L 63/14** (2013.01 - EP US); **H04L 63/1425** (2013.01 - EP US); **H04L 63/1433** (2013.01 - EP US); **H04L 63/20** (2013.01 - EP US)

Cited by

US10713586B2

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

WO 2017018926 A1 20170202; AU 2015403433 A1 20180208; AU 2015403433 B2 20210819; CN 106663169 A 20170510; CN 106663169 B 20210309; EP 3143547 A1 20170322; EP 3143547 A4 20171011; EP 3143547 B1 20190320; SG 11201509818U A 20170330; TW 201705034 A 20170201; TW I711938 B 20201201; US 10713586 B2 20200714; US 2017228658 A1 20170810

DOCDB simple family (application)

SG 2015050233 W 20150724; AU 2015403433 A 20150724; CN 201580004151 A 20150724; EP 15788313 A 20150724; SG 11201509818U A 20150724; TW 105107288 A 20160310; US 201514891621 A 20150724